CYBERSECURITY

Georgia election systems could have been hacked before 2016 vote

Georgia has been at the center of questions about voter security, due to the fact the state has used insecure paperless voting machines since 2002. | David Goldman/AP Photo

By KIM ZETTER
01/16/2020 11:07 PM EST

A Georgia election server contains evidence that it was possibly hacked before the 2016 presidential election and the 2018 vote that gave Georgia Gov. Brian Kemp a narrow victory over Democratic opponent Stacey Abrams, according to an election security expert.

The incident, which occurred in late 2014, long before either of those elections, not only calls into question the integrity of Georgia's voting machines during critical elections, but raises new questions about whether attackers were able to manipulate election data and voter information through the compromised server.

It's unclear who may have carried out the alleged attack or if voter information was altered, but Logan Lamb, the election security expert who uncovered the activity, believes that if hackers did breach the server, they could have gained "almost total control of the server, including abilities to modify files, delete data, and install malware."

Georgia has already been at the center of questions about voter security, due to the fact that the state has used insecure paperless voting machines since 2002.

Additionally, Georgia counties were among those that Russian hackers targeted in 2016 when they breached some state websites and probed others for vulnerabilities that would have given them access to voter registration databases and other election data and systems.

The Georgia server in question has been at the heart of a 2018 lawsuit brought by election integrity activists seeking to bar Georgia from using its paperless voting machines.

Lamb, who is an expert witness for the plaintiffs, uncovered the anomalies in an investigation for the plaintiffs. The allegation about the server, first reported by The Associated Press, were contained in an affidavit from Lamb filed Thursday in Atlanta federal court as part of the lawsuit.

Lamb declined to speak with POLITICO due to a court order, but one of the groups behind the case said his findings paint a disturbing picture about the state of elections in Georgia.

"It creates a very dark cloud over all of the previous elections because as we know there was no way to audit them, there was no ... attempt at accountability by the secretary of state, and the entire programming of elections was outsourced," said Marilyn Marks, executive director of the Coalition for Good Governance, one of the groups behind the lawsuit.

"[W]hat Logan's findings show us ... is that vulnerabilities were not just hypothetical as the state had been claiming. Now we know that it was a very real risk, but what we don't know is just how bad did it get. And the public deserves to know," she said.

Georgia used the server to distribute critical election and voter registration files to counties throughout the state. The state has insisted, however, that it never distributed files to program voting machines through the server. Instead, it delivered these files to counties physically. But if the server was compromised, it could have been a vehicle to distribute malware to any county election worker who connected to it.

Georgia's secretary of state, Brad Raffensperger, did not respond immediately to a request for comment. Kemp served as secretary of state at the time of the 2016 election, before being elected governor in 2018.

The Center for Election Systems at Kennesaw State University, which was responsible for programming all of the voting machines in Georgia before every election, owned and operated the server in question. That server was already known to have security issues.

As POLITICO first reported, months before the 2016 election, Lamb discovered that the KSU server was improperly secured so that anyone could access sensitive election data stored on it, and it also had an unpatched vulnerability in so-called Drupal software the server used, which would have allowed attackers to take control of the server and alter or delete data on it, or to post malware that could have infected the computers of election officials accessing the server.

Logan made the discovery by chance when he visited the Center for Election Systems website to learn more about their role in programming voting machines for Georgia.

After the POLITICO story published in June 2017, the plaintiffs filed their lawsuit and sought to obtain the server for evidence supporting their contention that Georgia's election systems are not secure and could have been tampered with in the 2016 election.

INTERACTIVE
How the Iowa caucuses work
BY BEATRICE JIN

But officials at Kennesaw wiped the server clean shortly after the plaintiffs filed their suit. The FBI had a mirror image of the server, which had been made in March 2017, but state officials fought to prevent the plaintiffs from obtaining it to examine. They lost that fight last year.

Only recently was Lamb able to examine the server for evidence of tampering. In his affidavit, Lamb said the server appears to have been compromised in December 2014, using an unpatched vulnerability called "Shellshock" that had been publicly revealed and widely reported three months earlier.

The Shellshock vulnerability is different from the Drupal one Lamb discovered when he visited the Center's website in 2016. Both the Shellshock and Drupal vulnerabilities had been publicly exposed around the same time, but despite both receiving extensive media coverage and even a Department of Homeland Security alert in the case of Shellshock, officials at the Center for Election Systems failed to apply a patch to close either of them when the patches were released.

Although a log on the server shows some of the alleged intruder's activity on it, there are signs the intruder may have deleted important information from the log, preventing Lamb from viewing everything that occurred.

A different log on the server that recorded access to the server's content-management system — the software the Center used to publish files and content on the Center's website for election officials to access — also thwarted Lamb's investigation because he had access to records going back to only Nov. 10, 2016, a few days after the 2016 election. This prevented him from seeing who might have accessed the content-management system prior to that date or altered its contents.

Lamb suggests in his court document that the logs were deleted intentionally and this was done for suspicious reasons.

"I can think of no legitimate reason why records from that critical period of time should have been deleted," he wrote.

But it's not uncommon for log files to record data for only a certain time period before they overwrite those records. Information about Drupal's access log published on a forum for Drupal developers and users indicates its access log saves data for only 16 weeks before deleting and overwriting it.

The other log Lamb was able to examine for the server itself does go back further, and this log shows that on Dec. 2, 2014, a new user named "Shellshock" was created on the server — the same name as the widely known vulnerability that was apparently used to get into the server.

About 15 minutes later, the log shows, the Shellshock vulnerability was patched on the server.

It's common for hackers to immediately patch the vulnerability they used to access a system, in order to keep other potential attackers out and maintain their control of the system. Although it could have been a system administrator who patched the server and created the Shellshock user account, a security expert told POLITICO it's unlikely.

"If I were a [system administrator], why would I create it and call it the same name as the [vulnerability]?" said Kevin Skoglund, an independent security expert. He said the suspicious name of the user account suggests the attackers may have been using automated software to scan for internet-connected servers containing the flaw. Once their malicious software found a vulnerable system, it may have been programmed to then automatically create a Shellshock user account on the system.

Lamb wrote in the court document that evidence in the log made it appear that the Shellshock user also tried to hide their activity once on the server. The log records a history of any commands initiated on the server, but it contained only a couple commands, suggesting the intruder may have deleted others.

There could be reasonable explanations for the suspicious activity Lamb spotted on the server.

"There may still be other explanations. It is possible, for example, that a CES employee" was the person behind the unusually named Shellshock account, he wrote in his court document.

But if a CES worker did apply the Shellshock patch in December, following the extensive media covered the Shellshock vulnerability had received three months earlier in September, it's odd that they didn't also patch the Drupal vulnerability that was publicly disclosed in October that year. The latter vulnerability was still on the server in August 2016 when Lamb visited it.

He believes the evidence points to an intruder.

"The long unpatched software, unusual username, potentially modified command history, and near immediate patching of the Shellshock bug are all strong pieces of evidence that an outside attacker gained access to the KSU server by exploiting the Shellshock bug," he wrote. Further investigation would need to be done to confirm this, he noted.

FILED UNDER: CYBER SECURITY, GEORGIA, ELECTION CYBERSECURITY